pwc

Secure cloud adoption:

A blueprint for financial services

Table of contents

01 Executive summary

02 Cloud adoption landscape in the Middle East

03 Data residency and sovereignty considerations

04 Strategic need for national-level cloud regulation

05 National secure cloud framework for the Financial Services sector

Executive summary

Driving secure cloud adoption in financial services

The financial services sector is undergoing a significant transformation, with cloud computing playing a crucial role in enhancing efficiency, scalability, and cost reduction. As competition intensifies, especially in a market where rapid responses to customer demands are vital, the adoption of cloud technologies is proving increasingly important.

The rapid advancement of cloud adoption in the financial services (FS) sector is accompanied by both opportunities and challenges for stakeholders and this includes national financial services regulators and cloud service providers. This paper explores the strategic importance of regulating secure cloud adoption, with a particular focus on the Middle East. Cloud computing is integral to the digital transformation of traditional banks, digital banks, insurance companies, fintech's and payment service providers. Hence, national regulators must play a central role in fostering a secure, compliant and efficient cloud ecosystem in their respective countries.

This paper examines current cloud adoption trends in the ME region, highlighting the challenges and risks associated with cloud deployments. Key concerns include data breaches, compliance gaps, insider threats and challenges faced in integrating legacy systems. The FS sector entities face significant security challenges in the cloud, necessitating a security-by-design approach to cloud migration, identity and access management, encryption, network security and continuous compliance monitoring. As cloud environments become more complex, the role of cloud-native security solutions, zero-trust architectures and AI-driven threat detection becomes critical to ensuring security and operational integrity.

Data residency and sovereignty are critical considerations in the region, influencing data movement restrictions and localisation requirements in various countries to ensure compliance with data sovereignty laws and navigate regulatory challenges.

This paper outlines a comprehensive framework for cloud-specific regulations, offering recommendations for central banks to facilitate secure cloud adoption. A well-structured regulatory framework is essential to address the concerns of FS sector entities, regulators, and cloud providers. This framework aligns with successful international regulatory models while being tailored to the unique needs of the Middle East region. By leveraging this framework, central banks and regulators can guide the secure journey of FS sector entities to the cloud, minimising risks and fostering innovation. Additionally, this framework provides actionable steps to help regulators establish a secure and compliant national cloud ecosystem for the financial services sector.

Key building blocks of secure cloud adoption framework

01 Regulatory governance and oversight

02 Cloud governance and leadership

03 Cloud operation and security

04 Data security

05 Monitoring and evaluation

Insights from cloud security breaches

High-profile breaches in the financial sector have underscored the importance of maintaining robust security measures in the cloud

01 Vulnerabilities in cloud-based infrastructure

Many of these incidents stemmed from vulnerabilities in cloud-based infrastructure or integrations with digital financial services platforms, such as SWIFT, and cloud-hosted applications.

02 Need for robust cloud security

These attacks highlight the need for cloud security measures, such as, data encryption, patch management, and access controls to protect sensitive customer information and ensure the continuity of financial operations.

03 Misconfigurations in third-party cloud services

Many breaches exploited vulnerabilities or misconfigurations in third-party cloud services (for example, cloud service providers, cloud-based API providers) used by financial organisations. This underscores the need for thorough third-party risk management and regular security assessments on cloud providers.

04 Shared responsibility model gaps

Security gaps can arise when financial organisations and cloud providers do not clearly define and implement their respective security responsibilities. Financial organisations must understand their role within the shared responsibility model, especially in managing data security and access controls.

05 Increased attack surface

As financial organisations rapidly migrate to the cloud for scalability, cost-efficiency, and flexibility, their attack surface expands and so does their exposure to cybercrime. Banks, credit agencies and other financial services, store vast amounts of sensitive data in cloud environments, making them prime targets for cyberattacks.

Cloud adoption landscape in the Middle East

Embracing the cloud

The financial sector in the Middle East is transforming, with cloud technologies emerging as pivotal drivers of growth and innovation. These advancements are reshaping the industry's landscape, positioning cloud solutions as strategic enablers of business transformation rather than merely tools for operational efficiency. By 2025, 75% of businesses in the region are expected to have adopted cloud solutions.[1]

Saudi Arabia

Cloud adoption rates in Saudi Arabia align with global trends, **with annual spending on public cloud services projected to reach US$3.9bn by 2027**, driven by an anticipated **CAGR of 23.4%** [13]

UAE

The public cloud services market in the UAE was valued at **US$2.2bn in 2023** and is projected to grow at **a CAGR of 21.7%, reaching US$5.9bn by 2028** [11]

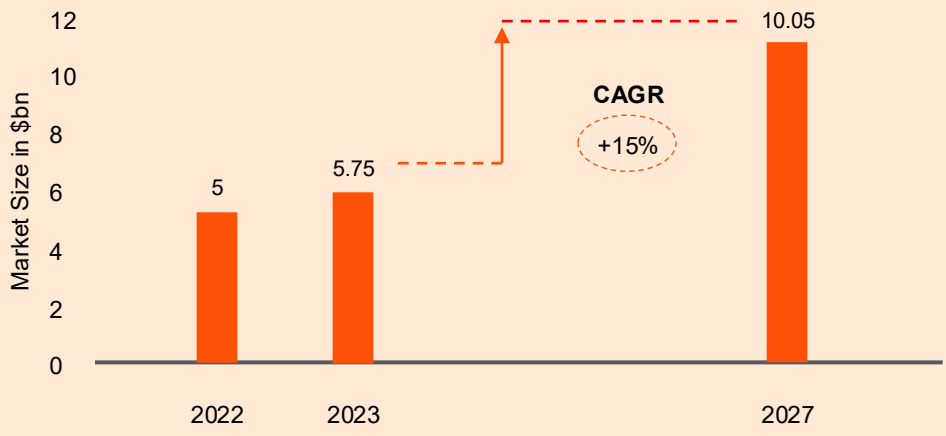
Qatar

In Qatar, the Public Cloud market is **projected to generate US$542.82m in revenue by 2025**, with Software as a Service (SaaS) leading the segment at US$197.46m, and the overall market is expected to grow at a **CAGR of 20.9% from 2025 to 2030, reaching US$1.4b by 2030** [12]

Overall, the Middle East's cloud services market is projected to grow at a CAGR of 15% from 2022 to 2027, reflecting increasing demand across industries, including financial services [1]

Cloud spending forecast in the Middle East

Middle East Cloud Market (2022-2027)



The increasing adoption of cloud technologies is largely influenced by ongoing digital transformation efforts and evolving regulatory landscapes. In Saudi Arabia, initiatives led by SAMA have been pivotal in encouraging the financial sector to adopt cloud solutions. Similarly, in the UAE, the Financial Services Regulatory Authority (FSRA) have created a supportive environment for digital banking and FinTech innovations, further propelling cloud adoption. The Qatar Central Bank, along with other regulatory institutions, has introduced clearer and more robust frameworks for cloud-based financial services, ensuring compliance and fostering trust. These regulatory developments, combined with a broader push for technological innovation, are reshaping the financial services landscape across the region.

Regulations enforcing cloud security controls in the Middle East are crucial for ensuring secure and compliant use of technology, especially in sensitive industries like the financial sector. The region is making significant progress in enhancing its cloud regulatory infrastructure to support digital transformation and secure cloud adoption in the financial sector. Various countries in the region have introduced frameworks and initiatives to promote data security, operational resilience, and compliance, fostering a secure environment for financial institutions.

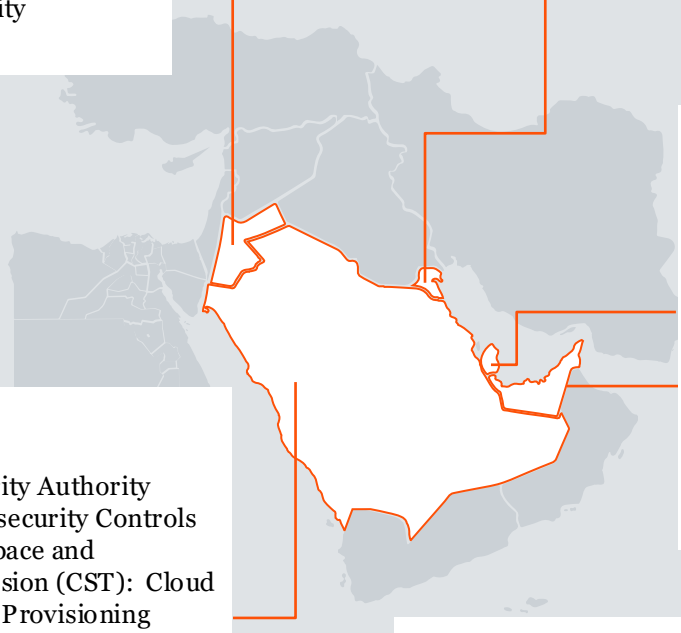
Key regulatory frameworks governing cloud security in the Middle East

Jordan

1. Central Bank of Jordan (CBJ): Cybersecurity Framework for Jordan Financial Sector
2. National Cyber Security Center (NCSC): Cybersecurity Framework Booklet

Kuwait

1. Central Bank of Kuwait (CBK): Cybersecurity Framework For Kuwait Banking Sector



Qatar

1. Central Bank of Qatar (QCB): CLoud Computing Regulation
2. Central Bank of Qatar (QCB): Information and Cybersecurity Regulation for Payment Service Providers
3. Central Bank of Qatar (QCB): Insurance Sector Cybersecurity Regulation

Saudi Arabia

1. National Cybersecurity Authority (NCA): Cloud Cybersecurity Controls
2. Communications, Space and Technology Commission (CST): Cloud Computing Services Provisioning Regulations
3. Saudi Arabian Monetary Authority (SAMA): Cybersecurity Framework
4. National Cybersecurity Authority (NCA): Essential Cybersecurity Controls

United Arab Emirates

1. Telecommunications and Digital Government Regulatory Authority (TDRA): UAE Information Assurance Regulation

This is not a comprehensive list of all regulations or guidelines governing cloud adoption in these countries or region.

Key implementation risks in cloud adoption

01 Lack of visibility and control

Inadequate cloud oversight can expose financial institutions to vulnerabilities and delayed incident responses, jeopardising data security and operational integrity.

02 Vendor lock-in and cloud portability

Financial institutions may face challenges with data migration and increased security risks due to a lack of system standardisation and portability between cloud providers.

03 Third-party risks

Third-party risks represent a significant challenge in cloud implementation because relying on external vendors for cloud services can expose organizations to security concerns and potential threats.

04 Inadequate cloud security configurations

Inadequate cloud security configurations can create vulnerabilities that expose systems and data to potential threats. Misconfigurations, such as open ports and default passwords, can compromise the overall security and reliability of the cloud environment.

05 Inadequate Identity and Access Management (IAM)

Inadequate Identity and Access Management (IAM) weakens control over access to cloud resources, increasing the likelihood of unauthorised access and security breaches. Effective IAM is essential to enforce least privilege and protect sensitive data in the cloud.

06 Complex integration requirements

Integrating cloud solutions with existing systems can lead to delays, higher costs, and operational disruptions. Compatibility challenges, data migration complexities, and the need for specialised expertise make the process resource-intensive and difficult to manage effectively.

07 Regulatory and compliance challenges

The dynamic nature of cloud services challenges financial services in maintaining compliance, as evolving regulations require rapid adaptation and significant resources.

08 Data breaches and unauthorised access

Data breaches and unauthorised access pose a major risk in cloud implementation, as transferring sensitive information can increase its exposure to unauthorised access if proper security protocols are not maintained.

As regulations evolve and more providers enter the market, adopting cloud services is becoming increasingly possible. However, the journey is filled with challenges that demand careful planning and execution. Among these, cyber risks stand out as a critical concern, the figure above highlights some of the key risks financial institutions should anticipate.

Secure cloud adoption: Best practices and approaches

Successful secure cloud adoption hinges on three pillars: robust governance, advanced technology, and a security-aware organisational culture. Effective cloud governance ensures that security is embedded from the outset - through a security-by-design approach - and is supported by comprehensive frameworks that enable ongoing compliance.

Organisations should adopt modern security technologies such as cloud-native security tools, zero-trust architectures, and AI-driven threat detection to proactively identify and mitigate risks. Just as critical is the human element: building a culture of security awareness and continuously upskilling employees through targeted training and development. Together, these integrated measures create a strong foundation for a secure, resilient, and compliant cloud environment.

Cloud governance

- ### Establish a national-level secure cloud adoption framework
  Define policies, roles, and responsibilities for secure cloud adoption at a national level. Ensure alignment with regulatory requirements, including data residency and sovereignty laws. The framework should cover the responsibilities of the financial service entities, cloud service providers and other key stakeholders.

- ### Embed security-by-design in the cloud migration journey
  Security must be embedded into every stage of the cloud adoption process, from planning to execution to termination. Employing structured frameworks to guide this integration ensures that security is treated as a core component rather than an afterthought. Organisations adopting a “security-by-design” approach experience fewer data breaches and improved compliance outcomes. This proactive stance enhances the overall cloud security posture, optimises performance, and promotes cost efficiency in cloud operations.

- ### Comprehensive risk assessments
  A comprehensive risk assessment is the cornerstone of any secure cloud adoption strategy. These proactive assessments identify vulnerabilities, threat vectors, and potential weaknesses within the infrastructure before cloud migration along with the potential third-party risks from CSPs. Early identification of risks significantly reduces the likelihood of breaches during migration. Necessary due diligence and safeguards need to be performed to avoid third-party risks and vendor lock-ins respectively.

- ### Continuous compliance monitoring and automation
  Develop a system for continuous monitoring and oversight of financial institutions’ cloud usage to ensure compliance with regulatory requirements. Implement auditing mechanisms to monitor cloud governance and usage by the financial institutions for compliance, ensuring transparency and accountability in data handling practices. Automated auditing tools streamline compliance efforts by real-time detections.

- ### Cloud Service Provider (CSP) certification
  The CSP certification from central banks and/or regulatory authorities helps to ensure that CSPs meet stringent security, compliance, and operational standards before offering their services to financial institutions. The certification process establishes a secure and trusted ecosystem where cloud services can be adopted without compromising data integrity, privacy, or regulatory compliance.

Role of cloud-native security solutions and zero-trust architecture

Cloud-native security solutions, such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), provide continuous visibility into cloud environments. CSPM tools help detect misconfigurations, while CWPP solutions secure workloads like containers and serverless applications. The Zero-Trust security model assumes that no entity - whether internal or external - should be trusted by default. Continuous access validation based on identity, device health, and context ensures a robust defense mechanism. Organisations adopting Zero-Trust architectures report fewer data breaches and improved security outcomes.

AI and machine learning in threat management

Artificial intelligence (AI) and machine learning (ML) are revolutionising cloud security by enabling real-time threat detection and response. These technologies analyse vast amounts of data to identify anomalies and potential threats, significantly reducing response times and mitigating risks. Predictive analytics adds another layer of sophistication, allowing organisations to forecast potential security incidents and implement preventive measures proactively. This approach is especially critical for countering advanced persistent threats (APTs).

Quantum computing on cloud encryption and security

Quantum computing poses a future challenge to traditional encryption methods, necessitating the adoption of quantum-resistant cryptographic algorithms. Organisations must begin integrating these algorithms to safeguard against emerging threats. Additionally, Quantum Key Distribution (QKD) offers an innovative solution for secure key exchange by leveraging quantum mechanics to ensure communication integrity. Though in its early stages, QKD is poised to play a crucial role in future cloud security strategies.

Data protection

Comprehensive encryption solutions safeguard sensitive data, ensuring compliance with regional data residency laws. These platforms offer secure key management and encryption technologies tailored to the specific needs of financial institutions in the Middle East. For example, an insurance company in the UAE implemented advanced encryption solutions to protect policyholder data, ensuring compliance with TDRA regulations. Additionally, the DLP technologies monitor and control data flows to prevent unauthorised sharing or exfiltration of sensitive data, especially in multi-cloud or hybrid environments.

Blockchain for data transparency

Blockchain technology provides a secure and transparent method for tracking data access and movement, ensuring compliance with residency laws. Blockchain can record the location of data storage and movement, ensuring adherence to data residency and sovereignty requirements in jurisdictions, such as the Middle East. Its immutable ledger enhances accountability and auditability, particularly in sectors such as financial services that require strict data integrity.

Strengthening identity and access management with RBAC and MFA

Implementing robust Identity and Access Management (IAM) controls combined with Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) forms a comprehensive security framework essential for protecting cloud environments. Centralised IAM tools streamline the management of roles and permissions across hybrid and multi-cloud environments, which is particularly effective in sectors with stringent regulatory requirements, reducing security vulnerabilities and ensuring compliance. RBAC enforces the principle of least privilege by restricting access based on specific roles and responsibilities, thereby minimising risks of insider threats and unauthorised access. Adding MFA as an additional layer enhances this security framework by requiring multiple forms of verification, effectively mitigating the risks associated with compromised passwords and credential theft.

People

- **Foster a culture of shared responsibility**
  Clearly define the roles and responsibilities of various personnel/stakeholders for the secure cloud adoption activities. Cloud security shall be a shared responsibility between the organisation, employees and cloud providers.

- **Training, upskilling and certifications**
  Conduct regular training and upskilling programmes to educate employees about secure cloud usage and handling sensitive data. Encourage staff to obtain relevant cloud certifications and ensure that employees are equipped with the necessary skills to manage cloud security effectively.

- **Cloud security champion**
  Ensure a cloud security officer or a champion is available to oversee cloud-related risks. The officer or the champion shall ensure the implementation of best practices across the entire cloud lifecycle within the organisation.

- **Nurturing cloud awareness**
  Creating a culture of security awareness is crucial for the successful implementation of cloud security measures. General awareness initiatives should focus on educating all employees about the importance of security and their role in maintaining it for cloud environments. Conduct phishing simulations to educate employees about recognising and responding to phishing attempts. This helps in reducing the risk of successful cyberattacks.

Data residency and sovereignty considerations

Implications of data movement restrictions and localisation

Data residency and sovereignty are critical considerations for cloud adoption, especially in regulated sectors like financial services, healthcare, government etc. Countries like Saudi Arabia, the UAE and Qatar have introduced stringent data localisation policies to safeguard national security, enhance compliance and preserve economic and cultural sovereignty. These regulations play a significant role in shaping cloud strategies and operational frameworks for businesses. The regulatory frameworks developed by authorities, such as the National Cybersecurity Authority (NCA) in Saudi Arabia and the Telecommunications and Digital Government Regulatory Authority (TDRA) in the UAE. The Qatar Central Bank (QCB) also mandates strict controls over how data is stored, processed, and transferred.

Data residency regulations mandate that sensitive data remain within the borders of the respective countries. This introduces complexities in cloud infrastructure management, as organisations must design systems that ensure compliance with local laws while maintaining operational scalability. For instance, storing sensitive financial or healthcare data locally may require significant investments in local data centres or forming partnerships with local service providers, which can increase costs and create operational inefficiencies. Additionally, these regulations restrict cross-border data movement, complicating global operations for multinational organisations. Businesses must navigate varying jurisdictional requirements, such as financial data residency rules in Qatar or healthcare data controls in Saudi Arabia while maintaining cloud strategies that foster innovation and efficiency.

While data localisation helps mitigate risks from cross-border data breaches, it also introduces localised vulnerabilities, such as, political instability, natural disasters and cybersecurity threats targeting specific countries or regions.

Adverse impacts of nonadherence with the data localisation and sovereignty laws could lead to:

- Legal repercussions and penalties
- Damage reputation and customer trust
- Operational challenges
- Exclusion from government contracts
- Barriers to entry
- Increased regulatory scrutiny
- Operational challenges

Adverse impacts of nonadherence with the data localisation and sovereignty laws could lead to:

01 Legal repercussions and penalties:

Non-compliance with data localisation laws in countries like Saudi Arabia, the UAE, and Qatar can lead to severe legal penalties, including hefty fines and sanctions. These nations enforce strict regulations to ensure that data generated within their borders is stored and processed locally.

02 Damage reputation and customer trust:

Entities that do not adhere to these laws risk significant reputational damage. This can erode trust among customers and business partners, which is essential for maintaining strong business relationships.

03 Operational challenges:

Failure to comply can result in operational disruptions, such as restricted access to data or the need to relocate data storage and processing facilities. These disruptions can be both costly and time-consuming.

04 Increased data security and privacy risks:

Storingstandards and potential vulnerabilities, increasing the risk of data breaches and cyber-attacks. data outside the jurisdiction can expose it to different security.

05 Increased regulatory scrutiny:

Non-compliant companies may face heightened scrutiny from regulatory bodies, leading to more frequent audits and inspections. This can divert resources from core business activities and increase operational costs.

06 Barriers to entry:

International cloud providers or businesses that don't follow localisation laws might be banned from entering the market or face restrictions in doing business with local entities.

07 Exclusion from government contracts:

In places like the UAE, failing to comply with data residency laws can disqualify businesses from bidding for government or public sector contracts, which are crucial for many companies.

Key best practices to adhere with data localisation and sovereignty laws

Adhering to data localisation and sovereignty laws is crucial for maintaining legal compliance, protecting business reputation, ensuring operational continuity, and safeguarding data security. Organisations can adopt the following strategies to effectively address data residency challenges while ensuring security and operational flexibility:

01
Adopt hybrid cloud models

02
Advanced encryption

03
Leverage local data centres

04
Adopt Cloud Access Security Brokers (CASBs)

05
Geofencing and access controls

06
Collaboration with regulatory authorities

07
Train staff on data residency requirements

01 Adopt hybrid cloud models

By 2027, 90% of enterprises will have adopted hybrid cloud architectures, as reported by Gartner in the Forecast: Cloud Computing, Worldwide, Nov 2024 report. A hybrid cloud approach has become an effective strategy for financial institutions in Saudi Arabia, Qatar, and the UAE to balance compliance with local data residency regulations while benefiting from the scalability and global reach offered by international cloud providers. For example, many large banks in the UAE use hybrid cloud solutions to store sensitive data locally while leveraging global public cloud resources for less-sensitive data and applications. Hybrid cloud models offer a balanced approach by combining the benefits of both private and public clouds. This flexibility is particularly beneficial for financial institutions that need to manage varying workloads and ensure high availability and disaster recovery.

02 Advanced encryption

Data encryption, both at rest, in transit, and in use, is essential for compliance with stringent Middle Eastern regulatory standards. For example, Saudi Arabia's NCA mandates robust encryption standards to protect critical financial data. Additionally, encryption of data in use, such as through homomorphic encryption, allows for secure processing of data without exposing it, further enhancing security. Financial institutions in Qatar, for instance, use end-to-end encryption to safeguard sensitive data stored in cloud environments while meeting QCB guidelines. In the UAE, financial institutions are required to implement advanced encryption techniques to protect customer data during transactions.

03 Leverage local data centres

Using cloud providers with data centres located within GCC countries ensures compliance with residency laws. For instance, cloud providers like Amazon Web Services and Microsoft Azure have established data centers in the UAE and Qatar, allowing organisations to store data locally and meet sovereignty requirements.

04 Adopt Cloud Access Security Brokers (CASBs)

CASBs provide visibility and control over cloud data, ensuring it remains within authorised jurisdictions. These tools help monitor and enforce data residency policies in line with NCA's Essential CybersecurityControls in Saudi Arabia and similar frameworks in the UAE.

05 Geofencing and access controls

Geofencing ensures data access is restricted to specific geographic regions, a critical measure for compliance with residency laws. Implementing robust access control mechanisms, such as role-based access control (RBAC) and multi-factor authentication (MFA), minimises the risk of unauthorised access and ensures sensitive data is securely managed. In Qatar, a leading insurance company implemented geofencing to restrict data access to within the country, ensuring compliance with local regulations.

06 Collaboration with regulatory authorities

Regular engagement with local regulatory bodies enables financial institutions to stay ahead of evolving compliance requirements. Proactively aligning cloud strategies with updates from bodies like the NCA, QCB, and TDRA can minimise disruptions and ensure long-term compliance. For instance, a fintech company in the UAE regularly consults with the TDRA to ensure their data management practices align with the latest regulatory standards.

07 Train staff on data residency requirements

Ensuring employees understand GCC data residency laws and their implications helps organisations maintain compliance. Regular training programmes help staff identify and avoid actions that could violate local data sovereignty laws, such as accidental cross-border data transfers.

Strategic need for national-level cloud regulation

Strategic need for national-level cloud regulation

Financial sector stakeholders, regulators, and cloud providers, often express strategic needs while adopting or implementing cloud technologies due to the critical nature of financial operations and the stringent requirements for protecting customer data. Cloud adoption introduces various complexities that demand careful attention, particularly in ensuring operational continuity, safeguarding sensitive financial information, and meeting regulatory compliance standards. Below are the key strategic considerations that these stakeholders typically evaluate when considering cloud technologies:

Key consideration	FS sector entities	Regulators	Cloud providers
01 Data privacy and security risks	The security of financial/customer data in the cloud is a key consideration due to the potential for reputational damage and legal consequences from breaches.	A key consideration is the need to update data privacy and security regulations to keep pace with the rapid advancements in cloud technologies.	Implementing security measures, including encryption, to ensure compliance with regulations and protect sensitive data.
02 Regulatory compliance	Regulatory compliance in cloud adoption is critical for financial institutions due to varying laws, risking legal issues and operational disruptions.	Responsible for enforcing local laws and ensuring organisational compliance with regulations.	Required to provide cloud services that align with the legal requirements of their operating jurisdictions, ensuring seamless regulatory compliance.
03 Vendor lock-in and interoperability	Intends to avoid any inability to switch cloud providers without incurring substantial costs or disrupting operations.	Dedicated to fostering fair competition in the market and discouraging dominance/monopoly by cloud providers.	Must offer interoperable solutions and avoid creating dependencies that lock customers into a single cloud ecosystem.
04 Cloud service reliability and performance	Requires the reliable performance and uptime of cloud services to ensure that critical financial services and customer transactions are not interrupted.	Monitor cloud providers to ensure they meet operational resilience standards and fair service-level agreements (SLAs).	Responsible for maintaining high availability and redundancy to ensure continuous service and performance.

Key consideration	FS sector entities	Regulators	Cloud providers
05 Integration with legacy systems	Potential challenges and considerations in integrating legacy infrastructure with modern cloud technologies, as it may delay cloud adoption and increase costs.	Oversee the integrity and security of legacy systems during cloud adoption to ensure regulatory compliance is maintained throughout the process.	Cloud providers need to offer integration tools and support to ensure that legacy systems are successfully migrated to the cloud with minimal disruption.
06 Data residency and sovereignty compliance	Storing sensitive financial data within the country or specific jurisdictions.	Focused on preserving local sovereignty over critical data and ensuring sensitive information remains within the respective national borders.	Must ensure that their cloud services comply with data residency laws and can store data in specific regions based on customer and regulatory requirements.

These challenges, mentioned above, underscore the importance of a comprehensive understanding of the risks and implications associated with cloud implementation.

National secure cloud framework for the FS sector

National secure cloud framework for the FS sector

The Central Banks could design and publish a comprehensive Secure Cloud Adoption Framework for the FS entities. This framework should help the central banks and regulatory bodies establish and enforce robust cloud security regulations. This framework ensures that the cloud adoption process in the FS sector is both secure and compliant with relevant regulations, providing clear guidelines for cloud service providers, financial institutions, and regulators to collaborate effectively.

This framework is structured around key domains and their corresponding sub-domains. Each domain addresses different aspects of cloud security, governance, and operational efficiency in a comprehensive manner. Below is a summary of the framework and how its components can drive secure cloud adoption in the FS sector.

1. Regulatory governance and oversight

National cloud governance	Innovation and collaboration	Cloud service provider certification	Regulatory oversight and audits	Continuous improvement

2. Cloud governance and leadership

Cloud Governance	Cloud Security Strategy & Architecture	Cloud Risk Management	Performance Management	Roles and Responsibilities
Staff Competence and Training	Secure Cloud Migration & Exit	CSP Due Diligence	Vendor and Contract Management	

3. Cloud operation and security

Forensic Readiness	Cloud Security Posture Management	Threat Intelligence	Asset Management	Real-time Security Monitoring
Physical Security & Equipment Redundancy	Patch Management	Advanced Threat Detection & Threat Hunting	Cloud Security Testing	
Identity & Access Management	Security Incident Management	Backup and Recovery Management	Cloud Security Testing	
Network & Perimeter Security	Secure Configuration & Isolation	Security Incident Management		

4. Data security

Data Governance	Data Protection	Data Residency	Data Sovereignty

5. Monitoring and evaluation

Legal & Regulatory Compliance	Regulatory Reporting	Exception Management	Internal Audit

01 Regulatory governance and oversight

This domain focuses on ensuring that the regulators maintain comprehensive oversight of cloud security policies and standards. It includes developing cloud governance frameworks at a national level, certification of cloud service providers (CSPs), and establishing regular audits to ensure ongoing compliance with security regulations. Continuous improvement of this framework and related cloud security measures is crucial for keeping up with evolving cyber threats. Collaboration between financial institutions, cloud providers, industry experts and regulators is key to fostering a secure cloud environment in the FS sector.

02 Cloud governance and leadership

The domain highlights the importance of defining/establishing a strong cloud security strategy and governance at the organisational level, supported by risk management practices. It guides the entities in establishing clear roles and responsibilities for cloud security management, ensuring staff are adequately trained, and facilitating secure cloud migrations. Additionally, it covers due diligence processes for selecting cloud service providers (CSPs) and managing contracts, ensuring that security and compliance requirements are met throughout the cloud adoption lifecycle.

03 Cloud operations and security

Focusing on the operational security of cloud environments, this domain outlines the processes for securing cloud workloads, applications, and data. It highlights the aspects to be considered while managing the entity's cloud security posture, implementing strong identity and access management, and conducting regular patch management. Moreover, it ensures that physical security and redundancy are in place to maintain cloud infrastructure resilience. Advanced threat detection, real-time monitoring, and incident management are also key aspects of maintaining a secure cloud environment. This domain is critical for ensuring that financial institutions' cloud environments are continuously monitored for security vulnerabilities and threats.

04 Data security

Data is a valuable asset in the financial services sector. Hence, it's crucial to ensure the protection and governance of sensitive data stored and processed in the cloud. Key aspects to be considered include implementing strong data protection measures, ensuring data residency or sovereignty compliance, and managing the flow of sensitive data within various cloud environments. By addressing these aspects, the framework helps financial institutions safeguard critical data while adhering to regulatory requirements related to data privacy and security.

05 Monitoring and evaluation

Regular monitoring and evaluation of the entity's cloud security practices by the regulators are vital for ensuring the effectiveness of cloud adoption in the FS sector. This domain covers the aspects to be considered in the legal and regulatory domains, ensuring that financial institutions and CSPs consistently meet security benchmarks. It also includes ongoing regulatory reporting, exception management, and internal audits to evaluate the adherence of the entities with the National-level Cloud Governance Framework. These efforts help ensure that cloud adoption remains secure and compliant on a long-term basis.

Case Study: Financial Conduct Authority's (FCA) role in shaping secure cloud adoption in the UK

Overview

The Financial Conduct Authority (FCA), established in 2013, is the UK's regulatory body responsible for ensuring market integrity, promoting fair competition, and protecting consumers. In 2016, the FCA introduced FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services. This guidance clarified regulatory expectations for securely adopting cloud services while managing associated risks, focusing on critical areas such as data security, operational resilience, and regulatory compliance. It provided financial institutions with clear measures to navigate challenges like data residency, security controls, and third-party accountability, enabling them to leverage cloud solutions without compromising their cybersecurity posture.

Key objectives of FCA guidance:

01 Clarify expectations:
Provide clear guidelines on the use of cloud services to ensure firms understand regulatory expectations.

02 Promote innovation:
Encourage the adoption of cloud technologies to foster innovation while ensuring customer protection by enabling firms to adopt secure, flexible cloud models.

03 Ensure operational resilience:
Maintain the resilience and security of firms' IT arrangements when outsourcing to cloud providers.

03 Encourage collaboration:
The guidance fosters transparency and collaboration between firms and regulators during audits or investigations.

04 Appropriate oversight and accountability:
Guidance also emphasises governance, ensuring institutions maintain oversight and accountability over outsourced activities.

Challenges

01 Implementation costs, estimated between £19.14m and £26.71m for one-off expenses, present a significant hurdle, particularly for smaller institutions.[7]

02 Underreporting of incidents persists, with only 2% to 2.5% of firms reporting operational incidents between 2018 and 2023, highlighting a need to further drive compliance efforts.[7]

03 Increasing complexity of risk management and compliance: Growing reliance on third-party providers has added complexity to risk management and compliance, especially for institutions operating across multiple jurisdictions.

04 Increased resource requirements:
Firms may face difficulties in allocating sufficient resources to implement FCA guidelines, manage ongoing operations, and pursue innovation concurrently.

Achievements

The FCA's guidance has delivered measurable improvements across several key areas. Financial institutions now conduct detailed risk assessments before engaging third-party IT services, enabling them to identify and mitigate cyber threats effectively. Additionally, ongoing monitoring ensures risks are managed dynamically. Data security has been strengthened with robust measures such as encryption, data residency policies, and breach notification processes, significantly improving data protection standards.

Operational incidents have been reduced due to clear directives on business continuity planning and recovery arrangements. Firms have also implemented and tested formalised exit strategies for seamless transitions without service interruptions. Governance has been improved through enhanced oversight of service providers, with firms retaining accountability for compliance and defining responsibilities for strategic and day-to-day management. Reporting efficiency has also increased, with firms saving approximately £270,000 annually due to standardised incident reporting processes that reduce follow-up clarifications.

The management of third-party risks has been strengthened by requiring firms to maintain and submit annual registers of material third-party arrangements. This has enabled the FCA to identify concentration risks and potential critical third parties (CTPs) to mitigate systemic vulnerabilities. Alignment with the international incident and third-party reporting frameworks such as Format for Incident Reporting Exchange (FIRE) and Digital Operational Resilience Act (DORA) has provided a consistent and globally recognised framework for cybersecurity and operational resilience.

A transformative initiative

The FCA's guidance for outsourcing to cloud and third-party IT services has proven to be a transformative initiative, significantly improving the cybersecurity and operational resilience of financial institutions. By focusing on risk management, data security, incident reporting, and governance, the FCA has created a framework that mitigates risks while enabling innovation. Although challenges such as implementation costs and reduced compliance persist, the long-term benefits of enhanced resilience and security far outweigh these obstacles.

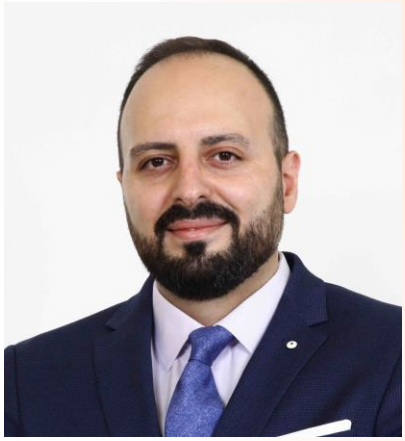
Looking ahead

Cloud computing offers unique benefits that can transform an entity's operations by enabling broader accessibility, on-demand self-service, and efficient resource management. As financial institutions in the Middle East continue to embrace these technologies, the regulators need to implement national-level secure cloud adoption frameworks to ensure that cloud environments utilised in the country are secure, compliant, and capable of supporting the growing needs of the financial services sector.

References

1. Cloud is the engine required to drive the next wave of innovation within Financial Services
2. One stop service of secure and compliant cloud tailored for the banking industry
3. 2024 Digital Trust Insights: Middle East findings
4. Your cloud transformation: Key accounting considerations and their broader impact
5. Cloud computing in the MiddleEast: New opportunities for companies and cloud providers
6. Time to raise the game in cloud: A strategic guide for Financial Institutions on the brink of transformation to capture cloud potential
7. FCA Operational Incident and Third Party Reporting
8. FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services
9. CISO Partner Solution Specialisations: Specialisations to transform infrastructure
10. Public cloud user spending to reach US$723bn in 2025
11. United Arab Emirates Public Cloud Market Forecast, 2024-2028
12. Public Cloud - Qatar
13. A cloud-powered future: Accelerating digital transformation in the Middle East

Contact us



Fady Chalhoub
Cybersecurity & Financial Services Leader
PwC Middle East
fady.chalhoub@pwc.com

Prasanth VS
Cybersecurity & Digital Trust
PwC Middle East
prasanth.vs@pwc.com